Chiffrement Inviolable

Par Amine CHBIHI MOUKIT

1- Problématique

Est-il possible de chiffrer un message par un code impossible à casser ? Oui, si et seulement si, nous pouvons inscrire le message à transmettre sur le support, une fois que celui-ci serait entre les mains du destinataire.

Nous proposons ci-après un dispositif, permettant d'envoyer un support d'information « vide » et d'y inclure l'information une fois le support arrivé à bon port.

2- Principe

Il s'agit de déterminer par la mesure si un flux de particules quantiques, que nous nommerons par la suite « baluchon de particules », a subi une réduction du paquet d'onde.

Pour cela nous proposons un dispositif expérimental qui nous informe si les particules d'un baluchon donné ont perdues leur nature ondulatoire.

le dispositif qui sera proposé, ne peut nous renseigner sur la réduction du paquet d'onde d'une seule particule, mais bel et bien d'un ensemble de plusieurs particules, 500 par

exemple, parvenant au dispositif de mesure les unes à la suite des autres, dans un laps de temps déterminé.

Il n'est pas essentiel que l'ensemble des particules d'un baluchon ait subi une réduction du paquet d'onde, mais uniquement une majorité, soit par exemple 90 %.

Par la suite le dispositif pourrait servir à identifier un code binaire comme suit :

1→ Baluchon à particules ayant subi une réduction du paquet d'onde

0→ Baluchon à particules n'ayant pas subi une réduction du paquet d'onde

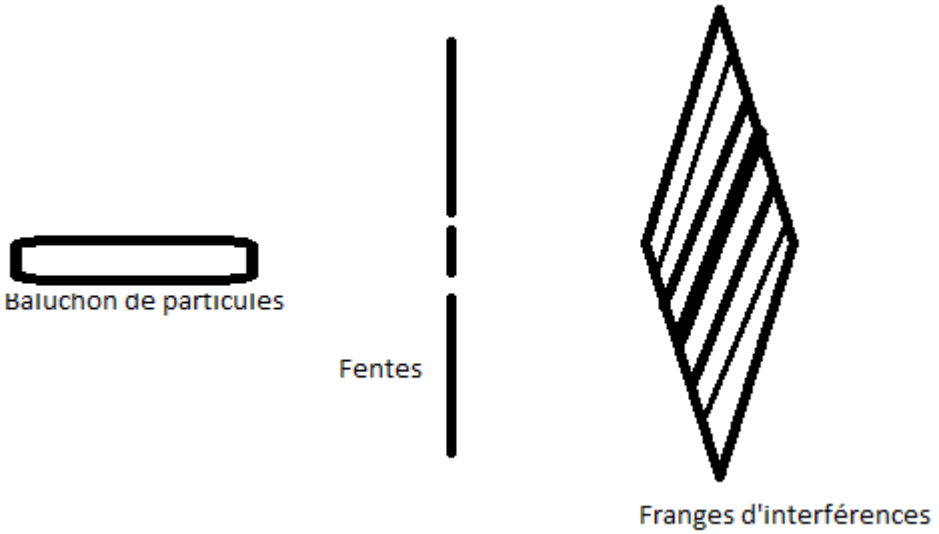
Ou vis versa.

Le nombre de particules (500) et le pourcentage (90%) sus-cités sont donnés à titre indicatif et seront affinés lors de la réalisation effective du dispositif.

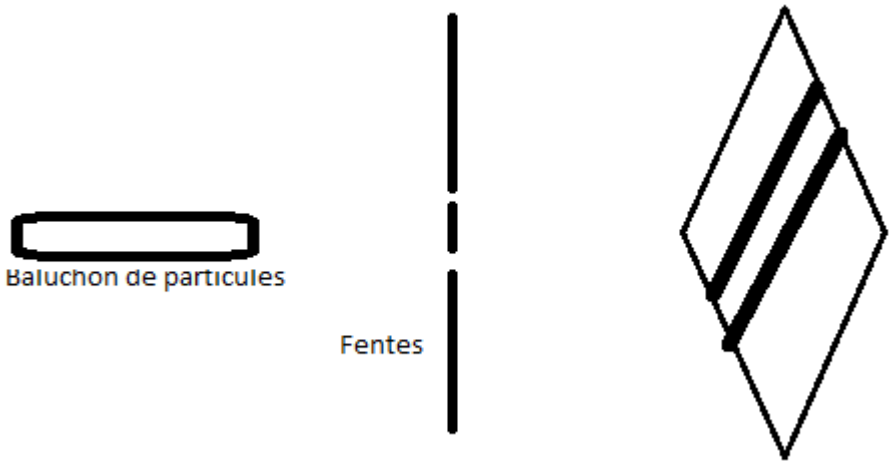
3- Dispositif

La détection se fera par le biais de deux fentes de Young couplées à une batterie de détecteurs.

En effet si nous recevons un baluchons de particule n'ayant pas subi de réduction de paquet d'onde, nous aurions comme résultat, sur un écran, des franges d'interférences : Figure1



Par contre pour les particules ayant subi une réduction du paquet d'ondes nous aurions le résultat suivant : Figure2

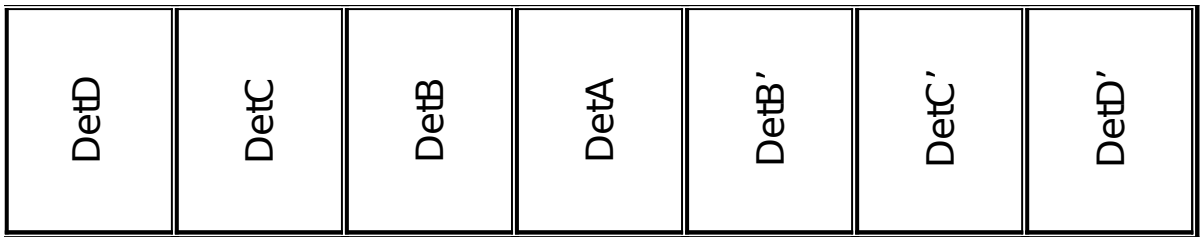


Remplaçons alors l'écran par une batterie de détecteurs de particules disposée selon les traces d'impacts sur l'écran et

à la même distance D des fentes que ne l'était l'écran des figures 1 et 2.

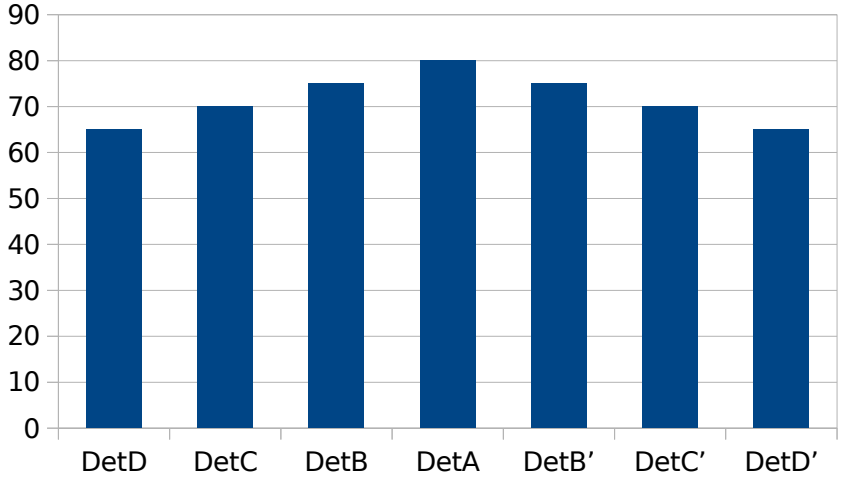
Appelons DetB et DetB' deux détecteurs placés aux lieux d'impact de l'ecran de la figure 2.

Appelons DetA, DetC, DetC', DetD et DetD' les détecteurs placés sur les autres traces d'impacts de la figure1.

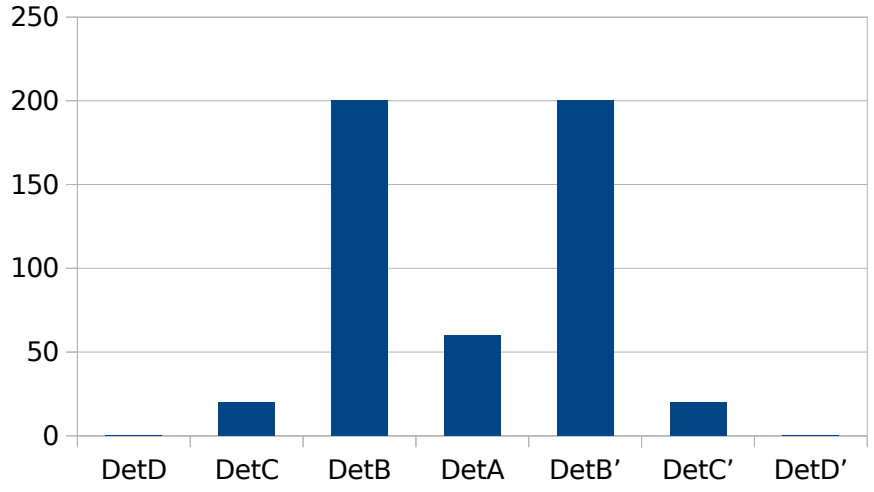


Nous obtiendrions approximativement alors les distributions suivantes :

a- **<u>Cas d'un baluchon de particules n'ayant pas subi de réduction de paquets d'ondes :</u>**



b**- Cas d'un baluchon ayant subi une réduction de paquets d'ondes :**

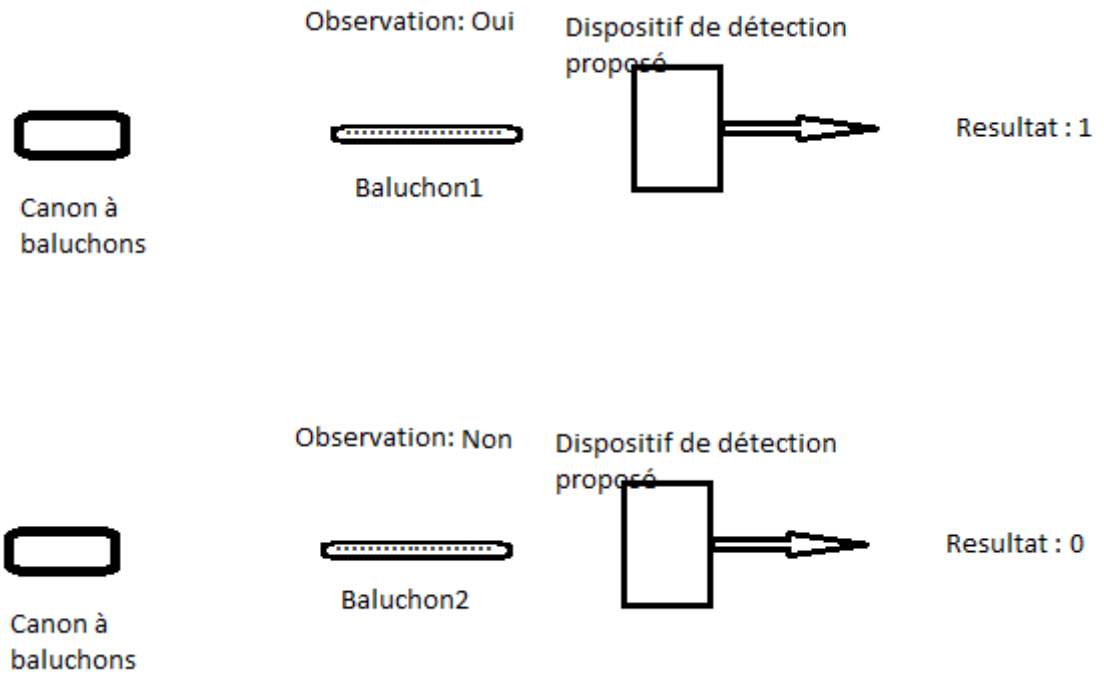


Bien entendu les deux distributions sus mentionnées sont données à titre uniquement indicatif de schématisation. Mais ce qui est certain c'est que le résultat des mesures sur la batterie de détecteurs sera différent selon que nous avons affaire à un ensemble de particules ayant subi une réduction des paquets d'ondes ou pas.

3- Déduction

Le dispositif sus-mentionné est en mesure de nous informer avec certitude si un ensemble de particules élémentaires a subi des mesures qui lui ont fait perdre le caractère ondulatoire par un phénomène de réduction du paquet d'onde.

Si ce dispositif est couplé avec un canon permettant des impulsions de baluchons de particules, un dispositif de mesure réduisant, ou pas, les paquets d'ondes des particules et une synchronisation avec un dispositif d'enregistrement des résultats des mesures sur la batterie de détecteurs, il est alors possible de matérialiser des messages binaires.



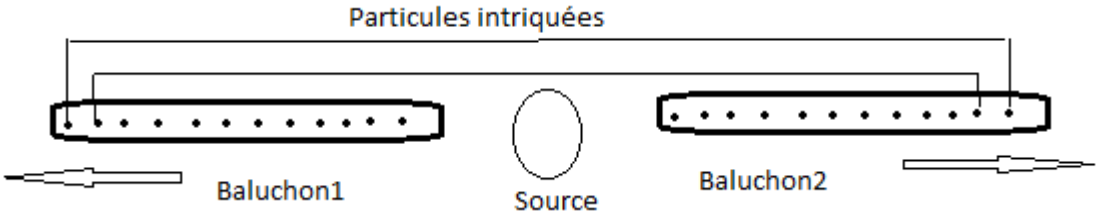
Maintenant imaginons que nous produisons des baluchons de particules intriquées deux à deux.

Si nous appliquons une mesure sur les particules du 1er baluchon de manière à réduire leurs paquets d'ondes, celles du deuxième baluchon subiront aussi une réduction instantanée de leurs paquets d'ondes. En détectant ces dernières par le dispositif ci-haut, nous aurions réalisé alors une transmission de l'information, à savoir qu'une action a été réalisée sur les particules du 1er baluchon et est détectable

par la mesure de la réduction du paquet d'onde des particules du baluchon2.

4- Application au chiffrement de l'information

Nous disposons d'une source d'électrons intriqués, permettant d'obtenir des baluchons de particules intriquées une à une :



Le baluchon2 est envoyé au destinataire du message tandis que le baluchon1 est gardé dans un dispositif cyclonique par exemple.

Une fois que la baluchon2 est arrivé à destination, nous appliquerons, ou pas, la réduction du paquet d'onde aux particules du baluchon1, immédiatement le résultat est détecté par le dispositif du destinataire.

Bien entendu, le dispositif de détection du destinataire, peut être activé par l'envoi d'abord d'une série préprogrammée de baluchons codé 1 (ayant subi une réduction du paquet d'onde), celui-ci répondra, par le biais d'un dispositif identique, confirmant la bonne arrivée des baluchons « messagers ».

Le vrai message parviendra par la suite, il ne contiendra une information qu'une fois arrivé à bonne destination, en effet chaque baluchon1 ne subira, ou pas, la réduction du paquet d'onde qu'une fois le baluchon2 correspondant(intriqué) parviendra à destination.

Ainsi l'interception en chemin, par espionnage, des baluchons messagers ne fournira aucun renseignement puisque ces mêmes baluchons ne portent pas encore d'information, d'où l'inviolabilité du chiffrement.